Privacy & Security Protection in an Online World

Philippa Lawson, Director
Canadian Internet Policy and Public Interest Clinic
University of Ottawa, Faculty of Law
www.cippic.ca

Insight Information Conference on Internet Law:
The Second Wave: New Developments, Challenges and Strategies
Toronto, Ontario
March 27-28th, 2008
Privacy vs. Security

• Privacy:
  – individual control over personal data
    • informed consent
    • openness
    • access to information + correction rights
  – limiting collection/retention
    • to what is necessary
  – limiting use/disclosure
    • to what was agreed
    • to what is reasonable
  – security safeguards
Statutory Security Requirements

- Private Sector
  - *PIPEDA*, Principle 4.8
  - Alta & BC *PIPAs*, s.34
  - Quebec Act, ss.10, 20

- Public Sector (Ont., Federal)
  - none in *Privacy Act*
  - Ontario *FIPPA* - Regs. 459, 460
Interpreting Security Req’ts

• B.C. Privacy Commissioner:
  – “The reasonableness of security measures and their implementation is measured by whether they are objectively diligent and prudent in all the circumstances.”
Security: Interpreting Req’ts

• Authentication
  – Industry Canada/Private Sector:
    • Principles for Electronic Authentication: A Canadian Framework (Ind Can; May 2004)
  – OPC:
    • PIPEDA #372, 299, 254
    • Guidelines for Identification & Authentication (Oct. 2006)
  – B.C.OIPC:
    • Determining Authentication Levels within the B.C. Government (March 2002)
Security – Interpreting Req’ts

• Computer security measures:
  – laptops
    • Alta OIPC - P2006-IR-005
  – public terminals
    • PIPEDA #177 – online banking kiosk
  – employee access
  – disposal
    • Ont. FIPPA Reg.459
    • Alta OIPC - P2006-IR-00
Security – Interpreting Req’ts

• Database protection
  – encryption standard
    • TJX/Winners – OPC/Alta OIPC Report (Sept ’07)
  – employee access

• Secure transmission
  – email (PIPEDA #360)
  – fax
  – mail
Other Statutory Security Reqs

• data minimization
  – limits on collection, retention
  – TJX/Winners: OPC/Alta OIPC Report (Sept’07)

• limits on use/disclosure
  – informed consent
  – reasonableness
Statutory Deficiencies

• No breach notification requirements
  – inadequate incentives for strong security
  – inadequate mitigation of damages

• No explicit limits on collection/use/disclosure of kids’ data
  – vague rule re: “appropriate purposes”

• Weak enforcement
  – inadequate incentives to comply with law
www.cippic.ca